UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/644,664	08/24/2000	Daniel T. Holland III	002.0141.01	5395

22895 7590 03/09/2004

PATRICK J S INOUYE P S
810 3RD AVENUE
SUITE 258
SEATTLE, WA 98104

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 03/09/2004

8

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/644,664	Applicant(s) HOLLAND ET AL.	
	Examiner Ellen C Tran	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 August 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 3.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Detailed Action

1. This action is responsive to communication: original application filed 24 August 2000, with the continuing date of 16 February 2000.

2. Claims 1-29 are currently pending in this application. Claims 1, 8, 15, 20, and 25 are independent claims.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-6, 8-13, 15-18, 20-23, and 25-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegel U.S. Patent 6,131,163 (hereinafter '163) in further view of Vaidya, U.S. Patent No. 6,279,113 B1 (hereinafter '113).

As to independent claim 8, "A method for intrusion detection data collection using a protocol stack multiplexor, comprising:" is taught in '163 col. 2, lines 4-12 "a system for evaluating data that arrives at a computer system that is executing a network operating system. The system comprises a protocol stack proxy";

"defining a hierarchical protocol stack within kernel memory space and comprising a plurality of communicatively interfaced protocol layers, each such protocol layer comprising one or more procedures for processing data packets; processing a data frame through the protocol stack, the data frame comprising a plurality of recursively encapsulated data packets which are each encoded with a protocol recognized by one of the

protocol layers" is shown in '163 col. 2, lines 23-33 "The system comprises a protocol layer proxy in a kernel memory of the network operating system and a sequence of instruction stored in the kernel memory configured to cause a processor under control of the network operating system to execute steps";

the following is not taught in '163:

- **"and collecting data directly from the protocol stack from at least one of the processed data packets using a protocol stack multiplexor, comprising:"** however '113 teaches "The reaction module 38 takes steps to trace the application session associated with the data packet" in col. 7, lines 7-10;

- **"interfacing directly into at least one such protocol layer through redirected references to the data packet processing procedures comprised within the at least one such protocol layer"** however '113 teaches "The virtual processor 36 communicates the server/application information to the configuration builder" in col. 7, lines 26-30;

- **obtaining a logical reference to the processed data packets from the interfaced protocol layer, the logical reference referring to a memory block in the kernel memory space within which the processed data packets are stored"** however '113 teaches "Extraction of the packet information enables the data collector 10 to detect network intrusions based in the different layer of the OSI model" in col. 7, lines 21-23;"

- **"and providing the logical reference to an intrusion detection analyzer executing within user memory space"** however '113 teaches "the virtual processor 36 notifies the reaction module 38, which then takes an appropriate action" in col. 7, lines 43-45.

- It would have been obvious to one of ordinary skill in the art at the time of the invention to modify intrusion detection system taught in '163 to include a means for collection data on the intrusion detected. One of ordinary skill in the art would have been motivated to perform such a modification because it would ease the burden of detecting intrusions by using lessons already learned see '113 (see col. 2, lines 53 et seq.) "What is needed is a network intrusion detection system which provides efficient extensibility to include newly discovered network attack signatures without substantially affecting performance of the network intrusion detection".

As to independent claims 1, this claim is directed to the system of the method of claim 8 and is similarly rejected along the same rationale.

As to independent claims 15, this claim is directed to a storage medium of the method of claim 8 and is similarly rejected along the same rationale.

As to dependent claim 9, "further comprising: providing a network hardware interface in a link protocol layer logically located at a device end of the protocol stack" is taught in '163 col. 2, lines 8-13 "The system comprises a protocol stack proxy coupled between a device driver on the computer system";

"providing an application software interface in a transport protocol layer logically located at a user end of the protocol stack" is shown in '163 col. 7, lines 4-9 "Each of the protocol layers comprises a software element or routine that can receive data organized according to particular protocol";

"and tapping the collected data from the protocol stack between and through the link protocol layer and the transport protocol layer" is disclosed in '113 col. 7, lines 31-34 "builer module 32 temporarily stores the applicable attack signature profiles in an instruction cache 42".

As to dependent claim 10, "wherein the protocol stack comprises a Transmission Control Protocol/Internet Protocol-compliant (TCP/IP) protocol stack" is taught in '113, col. 7 lines 21-33 "Extraction of the packet information enables the data collector 10 to detect network intrusions based in the different layers of the OSI model".

As to dependent claim 11, "further comprising: storing incoming data frames in a read queue associated with each protocol layer; storing outgoing data frame in a write queue associated with each protocol layer" is shown in '163 col. 7 lines 4-10 "Each of the protocol layers comprises a software element or routine that can receive data organized according to a particular protocol ... interpret the data in a network data packet, convert it to another protocol, and pass it onto";

"and retrieving the logical reference to the processed data packets from at least one of the read queue and the write queue" is disclosed in '113 col. 16, lines 12-17 "translating said attack signature profile into a set of instructions to be sequentially executed to enable recognition of a set of sequentially occurring events".

As to dependent claim 12, "further comprising: storing the references to the data packet processing procedures comprised within the at least one such protocol layer in a module switch table in the kernel memory space" is taught in '113 col. 12 lines 46-55 "storing a list of attack signature profiles descriptive of attack signatures associated with said network intrusion attempts";

"and replacing select procedure references in the module switch table with references to data collection procedures in the protocol stack multiplexor" is shown in '113 col. 16, lines 13-20 "translating said attack signature profile into a set of instruction to be sequentially executed to enable recognition of a set of sequentially occurring events which collectively constitutes said known network security violation" (i.e. "replacing" same as "translating").

As to dependent claim 13, "wherein one such protocol layer comprises a Transmission Control Protocol-compliant (TCP) protocol layer" is taught in '113, col. 7 lines 21-33 "Extraction of the packet information enables the data collector 10 to detect network intrusions based in the different layers of the OSI model";

"further comprising: augmenting the procedure references in the module switch table for the procedures for processing data frames for the TCP protocol layer with references to TCP data collection procedures in the protocol stack multiplexor" is shown in '113 col. 16, lines 13-20 "translating said attack signature profile into a set of instruction to be sequentially executed to enable recognition of a set of sequentially occurring events which collectively constitutes said known network security violation".

As to dependent claim 2-6 and 16-18 these claims incorporate substantially similar subject matter as in cited in the claims 9-13 above and are rejected along the same rationale.

As to independent claim 25, "A method for detecting network intrusions using a protocol stack multiplexor, comprising:" is taught in '163 col. 2, lines 4-12 "a system for evaluating data that arrives at a computer system that is executing a network operating system. The system comprises a protocol stack proxy";

"executing a network protocol stack comprising a plurality of hierarchically structured protocol layers, each such protocol layer comprising a read queue and a write queue for staging transitory data packets and a set of procedures for processing the transitory data packets in accordance with the associated protocol; interfacing a protocol stack multiplexor directly to at least one such protocol layer through a set of redirected pointers to the processing procedures of the interfaced protocol layer" is shown in '163 col. 3, lines 8-15 "According to another feature, the protocol layer proxy is coupled to a protocol stack of the network operating system and wherein one the security policies defines an acceptable criteria for data packets directed to";

"further comprising: referencing at least one of the read queue and the write queue for the associated protocol layer; and communicating a memory reference to each transitory data packet from the referenced at least one of the read queue and the write queue for the associated protocol layer" is disclosed in '113 col. 7, lines 7-45 "The reaction module 38 takes steps to trace the application session associated with the data packet";

"and receiving the communicated memory reference into an analysis module and performing intrusion detection based thereon" is taught in '113 col. 8, lines 53-56 "The different types of packet information enable generation of attack signatures profiles which can recognize network intrusions based on the different layers of the OSI model".

As to independent claims 20, this claim is directed to the system of the method of claim 25 and is similarly rejected along the same rationale.

As to dependent claim 26, "further comprising: storing a set of pointers to the processing procedures of the interfaced protocol layer into a module switch table; and

selectively redirecting the set of pointers to a set of data collection procedures comprised in the protocol stack multiplexor" is taught in '113 col. 16, lines 13-20 "translating said attack signature profile into a set of instruction to be sequentially executed to enable recognition of a set of sequentially occurring events which collectively constitutes said known network security violation".

As to dependent claim 27, "further comprising: redirecting the set of pointers for processing the transitory data packets for one of the read queue and the write queue for the; associated protocol layer" is shown in '113 col. 14, lines 16-24 "further comprising an intrusion detection alert mechanism in communicative contact with said processing means, said detection alert mechanism being configured to perform a predetermined act if said processing said attack signature profile reveals a network intrusion, said predetermined act being one of alerting a network administrator denying access".

As to dependent claim 28, "further comprising: redirecting the set of pointers for processing the transitory data packets for both the read queue and the write queue for the associated protocol layer" is disclosed in '113 col. 14, lines 16-24 "further comprising an intrusion detection alert mechanism in communicative contact with said processing means, said detection alert mechanism being configured to perform a predetermined act if said processing said attack signature profile reveals a network intrusion, said predetermined act being one of alerting a network administrator denying access".

As to dependent claim 21-23 these claims incorporate substantially similar subject matter as in cited in the claims 26-28 above and are rejected along the same rationale.

5. Claims 8, 14, 19, 24, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over '163 in further view of '113 in further view of Shanklin et al. U.S. Patent No. 6,489,666 B1 (hereinafter '666).

As to dependent claim 14, the following is not taught in the combination of teachings of '163 and '113:

- **"wherein one such protocol layer comprises a User Datagram Protocol-compliant (UDP) protocol layer"** however '666 teaches "the packets incoming to local network 10 may adhere to various protocols running on top of the IP protocol or to IP extensions. For example, the IP protocol may have a TCP or UDP protocol ... The UDP (user datagram protocol) is used primary for bradcasting messages" in col. 3, lines 35-43;

- **"further comprising: replacing the procedure references in the module switch table for the procedures for processing incoming data frames for the UDP protocol layer with references to UDP data collection procedures in the protocol stack multiplexor"** however '666 teaches "further comprising the step of transforming said regular expression to a decision tree" in col. 7 lines 18-19.

- It would have been obvious to one of ordinary skill in the art at the time of the invention to modify intrusion detection system with collecting data directly from the protocol stack taught in the combination of teachings '163 and '113 to include a means for replacing or redirecting references collected. One of ordinary skill in the art would have been motivated to perform such a modification because to properly detect intrusions it requires procedures that require the ability to apply modifications see '666 (see col. 1, lines 61 et seq.) "For signature indicted by a single packet, the detection process can be as simple as matching a binary string of

an incoming packet to a stored binary string. However, for composite signatures, the detection process often requires the use of procedural code, involving loops, count, comparisons and other processing mechanisms".

As to dependent claim 7 and 19 these claims incorporate substantially similar subject matter as in cited in the claim 14 above and are rejected along the same rationale.

As to dependent claim 29, "wherein the network protocol stack is a TCP/IP-compliant protocol stack, further comprising: defining a set of TCP/IP -compliant protocol layers, selected from the group comprising at least: a data link protocol layer; an Internet (IP) protocol layer; an Transmission Control Protocol (TCP) layer; and a User Datagram Protocol (UDP) layer wherein one such protocol layer comprises a User Datagram Protocol-compliant (UDP) protocol layer" is taught in '666 col. 3, lines 35-43 "the packets incoming to local network 10 may adhere to various protocols running on top of the IP protocol or to IP extensions. For example, the IP protocol may have a TCP or UDP protocol ... The UDP (user datagram protocol) is used primary for bradcasting messages".

As to dependent claim 24 this claim incorporate substantially similar subject matter as in cited in the claim 29 above and are rejected along the same rationale.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (703) 305-8917. The examiner can normally be reached on 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-5484.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Ellen Tran
Patent Examiner
Technology Center 2134
2 March 2004